DOI 10.37882/2223-2966.2024.06.36

ОПТИМИЗАЦИЯ ОЦЕНКИ РИСКА ДЛЯ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ С ИСПОЛЬЗОВАНИЕМ ИНТЕЛЛЕКТУАЛЬНОЙ МОДЕЛИ, ОСНОВАННОЙ НА НЕЧЕТКИХ ЛОГИЧЕСКИХ ВЫВОДАХ ВОЗОБНОВЛЯЕМЫХ ПРАВИЛ

OPTIMIZATION OF RISK ASSESSMENT TO SUPPORT DECISION MAKING USING AN INTELLIGENT MODEL BASED ON FUZZY LOGICAL INFERENCE OF RENEWABLE RULES

D. Suzdalsky

Summary. The unreliability of wired communications and the risks of controlling the data transfer process, as well as the complexity affecting data protection and the high costs of system infrastructure, have led to the use of wireless communications. However, these networks are vulnerable to cyber-attacks. The side effects of these attacks are changing data or penetrating the security system and exposing its weaknesses, which leads to large losses. These risks and complexities have led to the move away from wired communications and towards the adoption of smart techniques and strong encryption algorithms to protect against cyber-attacks. The article presents a scenario for intelligent technology to improve the reliability of data transmission and proposes a new way to increase the level of protection, as well as reduce infrastructure costs.

Keywords: encryption key, encryption, fuzzy, risk assessment, WLAN.

Суздальский Дмитрий Андреевич
аспирант, Российский экономический университет им. Г.В. Плеханова
t7699690@gmail.com

Аннотация. Ненадежность проводной связи и риски контроля процесса передачи данных, а также сложность, влияющая на защиту данных, и высокие затраты на инфраструктуру системы привели к использованию беспроводной связи. Однако эти сети уязвимы к кибератакам. Побочными эффектами этих атак являются изменение данных или проникновение в систему безопасности и обнаружение ее слабых мест, что приводит к большим потерям. Эти риски и сложности привели к отказу от проводной связи и применению интеллектуальных методов и надежных алгоритмов шифрования для защиты от кибератак. В статье представлен сценарий интеллектуальной технологии для повышения надежности передачи данных и предложен новый способ повышения уровня защиты, а также снижения затрат на инфраструктуру.

Ключевые слова: ключ шифрования, шифрование, нечеткий, оценка риска, WLAN.

Беспроводные сети имеют наибольшие преимущества по сравнению с проводными сетями, особенно после роста спроса на использование информационных ресурсов для поддержки принятия решений, таких как способность передавать значительные объёмы данных в приложениях реального времени. Однако беспроводные технологии также создают новые проблемы в передаче данных. В отличие от проводных сетей, беспроводные сети передают данные, используя радиочастотную или инфракрасную передачу. Используемая в настоящее время беспроводная технология позволяет злоумышленнику контролировать беспроводную сеть и в худшем случае может повлиять на целостность данных. Вышеупомянутые уязвимости и угрозы, возникающие при адаптации беспроводной связи, очень важны для обеспечения безопасности беспроводной сети, будь то домашняя или корпоративная сеть [1]. Это позволит снизить риски для данных пользователей, использующих эти коммуникации. Чтобы преодолеть эти риски, предлагается фреймворк применения интеллектуального шифрования с надежной методологией классификации для максимизации аутентичности. Шифрование — это ключ к обеспечению большей безопасности информации в сети Wi-Fi. Однако широко используемые известные методы шифрования имеют большие недостатки и уязвимы для злоумышленников из-за нарушения конфиденциальности и рисков [2]. Данные WEP передаются в 64-битном или 128-битном формате [3], но фактические ключи передачи имеют длину 40 бит или 104 бита, а остальные 24 бита представляют собой вектор инициализации (Initialization Vector, IV) для отправки в пакете вместе с данными [4].

Организация должна осуществлять непрерывный мониторинг атак и уязвимостей, а также проводить периодическую техническую оценку безопасности для мониторинга общей безопасности беспроводных локальных сетей (WLAN) [5]. Использование надежных стандартов шифрования защищает сети WLAN от самых серьезных угроз [6]. Этот метод обеспечивает новую

методологию создания интеллектуальной и самоадаптирующейся системы, основанной на создании возобновляемого правила и шифрующей данные, когда они находятся на высоком уровне риска. Такой подход является самым простым, если принять во внимание как простоту управления распределением ключей шифрования, так и снижение стоимости инфраструктуры для защиты передаваемых данных, а также достижение максимальной степени параметров шифрования (т.е. безопасности, надежности и аутентичности). Его конструкции способны снизить риски в различных ситуациях, например, шум, который влияет на точность данных, отправляемых за счет использования концепций нечеткой схемы, чтобы снизить все возможные уровни риска. Целью различных связанных методов является обеспечение безопасности данных, передаваемых через беспроводные сети, поэтому Sedghi и Kaghazgaran [7] вводят криптографию с открытым ключом для обеспечения безопасности беспроводной сети.

Нечеткая логика и оценка риска

Нечеткая логика — это часть искусственного интеллекта (ИИ), которая пытается решить проблему с помощью человеческого интеллекта [8, 9]. Оценки рисков в формате нечеткой логики определяются набором логических правил. Результаты оценки риска с помощью нечеткой логики облегчают принятие решений [10]. Создание системы нечеткого вывода включает в себя систему правил, которая определяет, как выходные данные выводятся из данных нечетких входных данных [11].

Для поддержки принятия решений уникальный метод правильного прогнозирования риска деятельности заключается в сборе как можно большего количества связанных исторических данных и анализе корреляции между особенностями, которые способствуют возникновению деятельности [12]. Обучение нечетким правилам в нечеткой системе поддержки принятия решений включает знания при проектировании системы, отношения ввода-вывода которой определяются набором нечетких правил [13, 14]. Теория многокритериального решения предполагает, что лицо, принимающее решение (ЛПР) полностью рационально в выборе оптимального решения [15]. Мультиагентная технология, являющаяся частью области искусственного интеллекта, также может использоваться для интеллектуальной оптимизации [16].

Оценка риска — это процесс выявления, анализа и оценки риска. Идентификация риска включает понимание источников риска и возможных проблем [17]. Функции принадлежности связаны лингвистическим союзом: «и» (для максимизации) и «или» (для минимизации). Для задачи максимизации степени принадлежности в множестве решений для оптимального решения формулируется [17]:

$$x^* = \arg[\max \min\{\mu G(x), \mu c(x)\}], \quad (1)$$

где G — цель, а c — ограничения. В то время как оптимальное решение через наименьшую степень принадлежности во множестве решений выглядит следующим образом [17]:

$$x^* = \arg[\min \max\{\mu G(x), \mu c(x)\}], \quad (2)$$

Минимизация рисков и оптимизация управления передаваемых пакетов является основной целью данного исследования. Благодаря характеристикам безопасности и надежности системы это исследование охватывает все риски ожидаемых катастроф безопасности в нескольких обстоятельствах. Было использовано наблюдение за сетью и выявление поведения злоумышленников посредством неконтролируемого обучения. Характеристики извлекаются и оцениваются после сбора данных для проверки передаваемых пакетов.

Прежде всего, основным ядром этого шага является создание нечетких правил для создания базы знаний для правил риска, которая была сформирована с помощью двух конкретных моделей следующим образом. Первый модуль представляет собой построение базы знаний о рисках. Этот модуль направлен на создание хранилища уровней риска и предметно-ориентированных решателей из части вывода для многих рисков и сосредоточения внимания на причинно-следственных связях на основе их знаний [18]. Целью второго модуля является модель результатов оценки рисков (т. е. поток в процессе принятия решений о рисках, и результаты решения возвращаются в систему для уточнения нечетких множеств и правил. Модели нечеткой логики, используемые с другими моделями риска, такими как деревья решений для моделирования сложных проблем риска). В предлагаемой системе шифрование пакетов должно быть решено с приведением к их типу. Ключевой особенностью нечетких множеств является отсутствие жестких правил определения их функций принадлежности [19]. Чтобы установить правила вывода из нечетких данных в системе безопасности WLAN, выбираются независимые и зависимые переменные, а затем принимаются нечеткие множества с числовыми значениями. В этом исследовании данные являются зависимыми переменными, а истинные пакеты — независимой переменной.

В работе предложен алгоритм, обеспечивающий достижение двух важных функций: i) безопасности данных и обеспечения их надежности и ii) создания регистрирующей автоматизированной системы безопасности. При этом используется метод, обеспечивающий более высокую безопасность передаваемых данных, которые формируются в виде пакетов. Алгоритм можно уточнить следующим образом:

а. Начальный ключ (базовый ключ) заявлен и представлен сдвиговым регистром в виде 16-битного (два байта).

б. Ключ сообщения (64 бита), представленный (4 сдвиговыми регистрами).

в. Каждый бит ключа сообщения интегрируется с выходными данными сдвигового регистра для основного ключа в соответствии со следующей последовательностью нелинейной функции:

$$Output = B_k \oplus M_k \oplus \wedge I_k \cdot \quad (3)$$

д. Указание случайной перестановки для вывода.

е. Окончательный вывод будет организован с использованием математической формы:

$$O_f = output_n \oplus\sim (P_k),$$

где P_k — бит пакета.

Получатель расшифровывает зашифрованные пакеты с помощью обратного цикла предложенного алгоритма, который показан на рисунках 1 и 2 соответственно. На рисунке 1 представлена обобщенная блок-схема предлагаемой системной архитектуры, в которой для классификации пакетов использовался наивный байесовский классификатор и генератор возобновляемых правил с базой уровня риска для оптимизации оценки риска.

Предлагаемые правила и математическая гипотеза используются для улучшения и введения фактов и правил с помощью логической и дискретной теории. Индуктивные правила: modus ponens, modus tollens, сложение, упрощение, гипотетический силлогизм, дизъюнктивный силлогизм и разрешение. Модели правил рассуждений вывода определяют правила предлагаемой системы.

Анализируя данные, можно выделить четыре переменных параметра QoS. Они включают задержку, колебания задержки передачи пакетов, потерю пакетов и про-

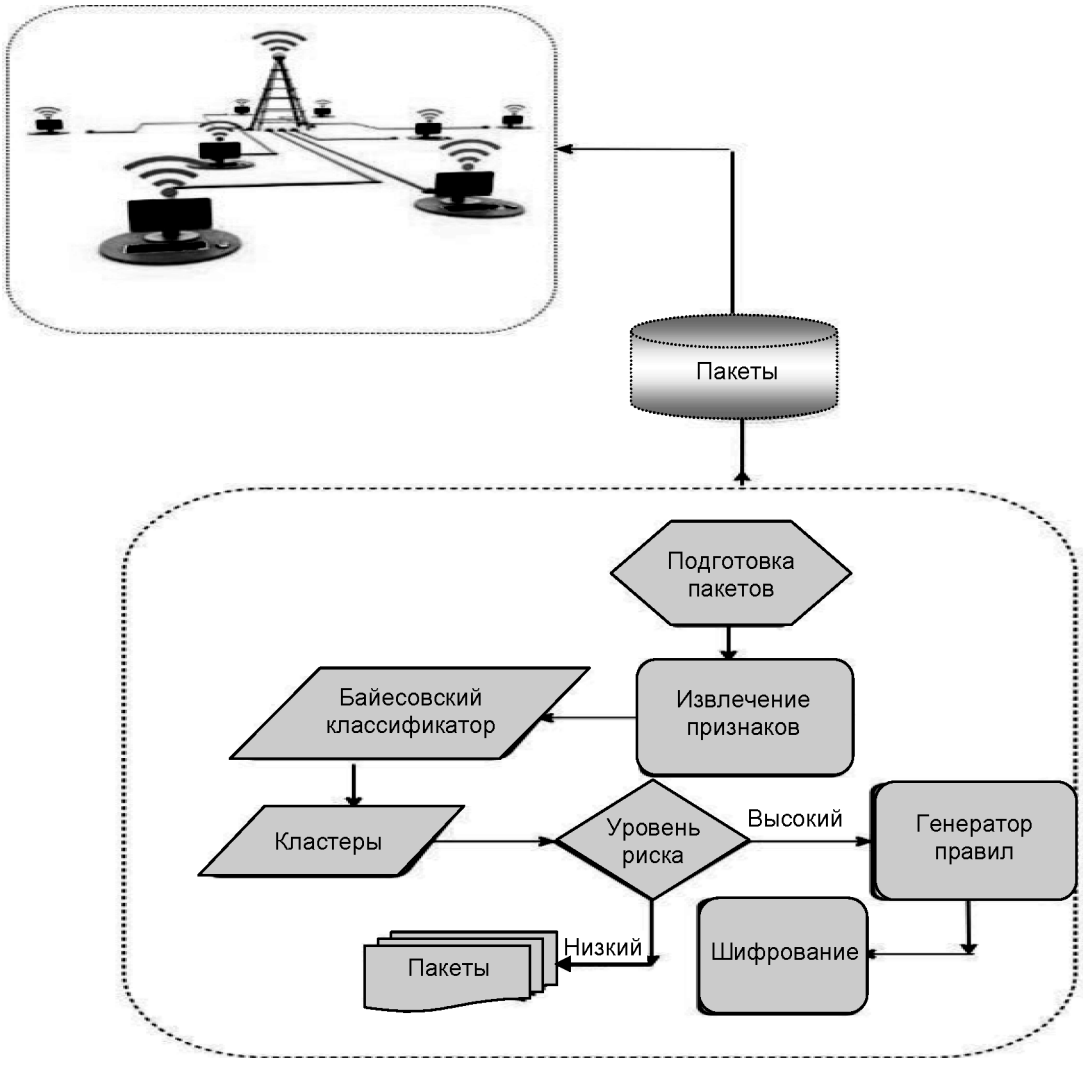

Рис. 1. Блок-схема предлагаемой системы

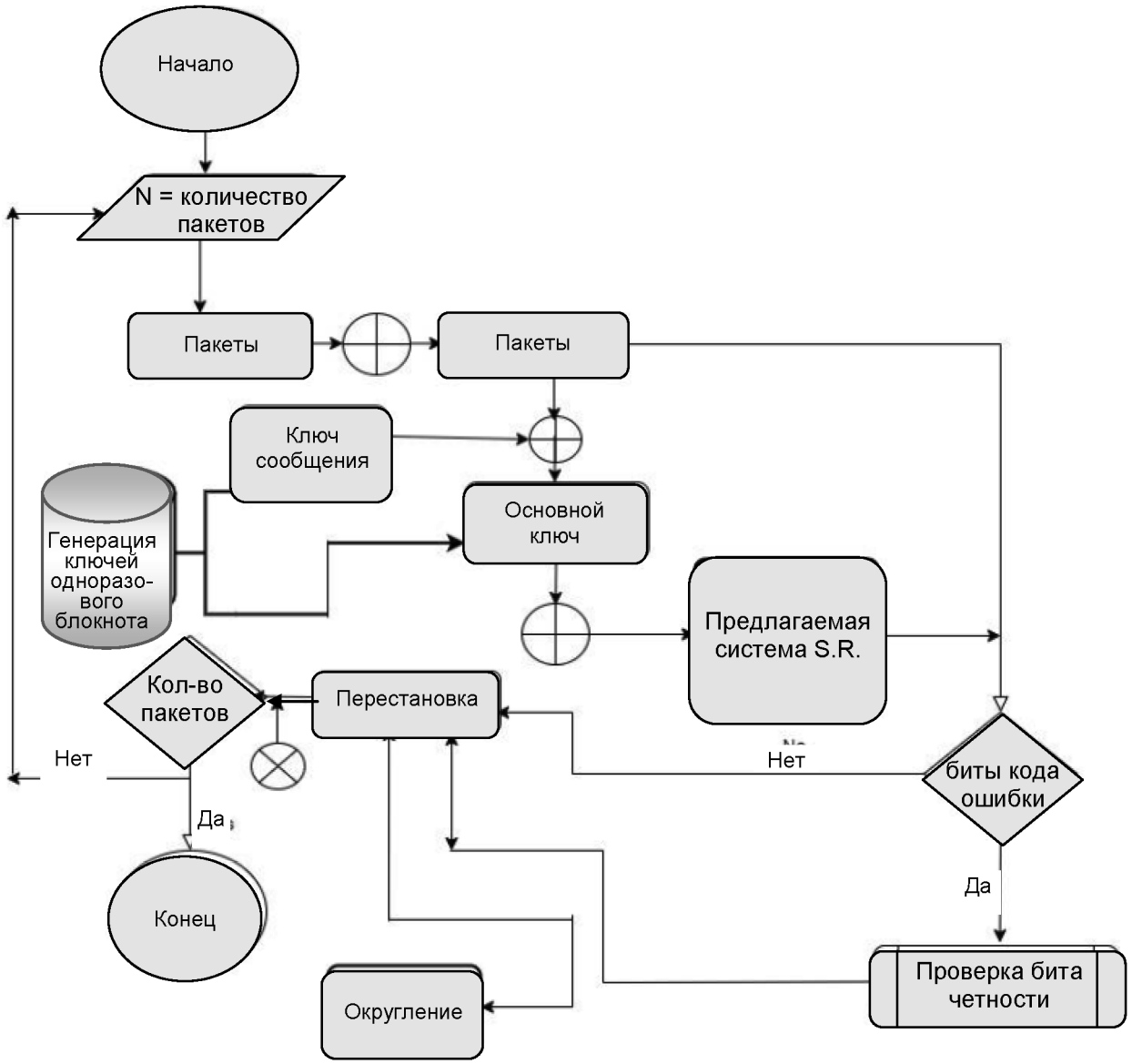

Рис. 2. Предлагаемая система с контролем безопасности

пускную способность. Метод анализа данных о качестве IP-сети реализован путем расчета значения каждого параметра качества обслуживания, такого как коэффициент задержки, который представляет собой количество задержек, разделенное на количество принимаемых пакетов, и процент потери пакетов [21], как показано в (4):

$$percentage\ \ Packet\ \ Loss = \frac{\left(Number\ \ of\ \ sent\ \ packets - Number\ \ of\ \ received\ \ packets\right)}{Number\ \ of\ \ sent\ \ packets} \times 100 \quad (4)$$

$$Throughput = \frac{Number\ \ of\ \ Packets \times 8}{Simulation\ \ time} \quad (5)$$

Предлагаемая система достигает этих параметров качества обслуживания для передаваемых пакетов после оптимизации риска, как неявно показано ниже в таблицах 2 и 3.

В качестве классификатора можно использовать наивный Байес классификатор, основанный на статистической теореме Байеса и атрибутах и гипотезах независимости. Это описательный метод и независимая модель признаков. Наивные байесовские классификаторы можно очень эффективно обучать на обучающем наборе с учителем. Для оценки параметров используется метод максимального правдоподобия. На рисунке 3 представлены каскадные этапы этого метода, где вероятность классификации можно определить с помощью (6).

$$P\left(H|X\right) = \frac{P\left(X|H\right)P\left(H\right)}{P\left(X\right)}, \quad (6)$$

где $P(H|X)$ — апостериорная вероятность H, обусловленная X. Напротив, $P(H)$ — априорная вероятность H. Аналогично, $P(X|H)$ — апостериорная вероятность X, обусловленная X. H. $P(X)$ — априорная вероятность X.

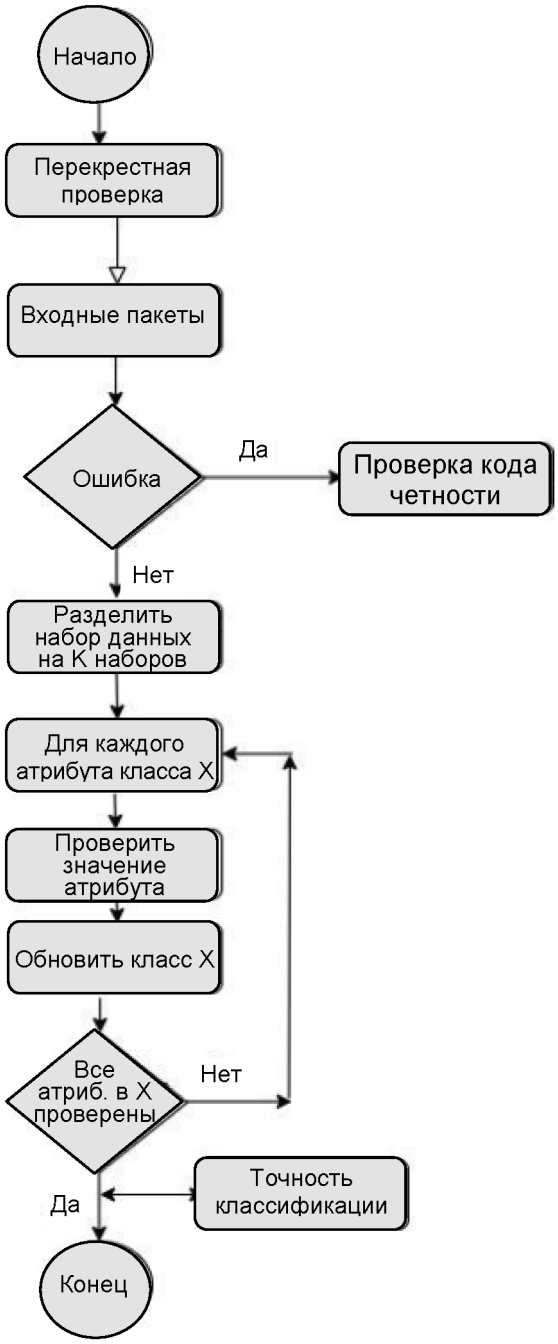

Рис. 3. Наивный байесовский классификатор

Это метод оценки значений параметров $\theta = (K,(n)k,hk)$, который основан на информации из данных yn (выраженной в распределении вероятностей $f(y|\theta)$) и информации о параметре θ (выражается в априорном распределении $\pi(\theta)$) [22].

Оценка риска является целью данного исследования, так что задачей предлагаемого метода является максимизация надежности и конфиденциальности данных и сети за счет снижения и минимизации уровня риска. В таблице 1 представлена оценка рисков и правил, где есть три параметра для назначения шифрования с использованием предложенной модели, управляемой и контролируемой через порог. Порог указан, изменен и обновлен в соответствии с конфиденциальностью данных и размером пакета. Итак, управление рисками — это идентификация, оценка и приоритезация рисков (путем измерения рисков) с последующей координацией и экономичным применением ресурсов для минимизации, мониторинга и контроля вероятности и/или воздействия неблагоприятных событий (путем обработки рисков) [23].

Таблица 1.

Оценка рисков и правил

Размер пакетов	Риск	Шифрование
Малый	Низкий	Негативное
Большой	Низкий	Позитивное
Малый	Средний	Негативное
Большой	Средний	Позитивное
Малый	Высокий	Негативное
Большой	Высокий	Позитивное
Малый	Очень Низкий	Негативное
Большой	Очень Низкий	Негативное
Малый	Очень Высокий	Негативное
Большой	Очень Высокий	Позитивное

Таблица 2.

Принятие решений и тип атаки

Тип атаки	Размер пакетов	Порог риска	Уровень риска	Шифрование (Решение)
Маскировка	Малый	0,213	Низкий	Негативное
Фальшивая точка доступа	Большой	0,681	Низкий	Позитивное
MITM	Малый	0,114	Средний	Негативное
DOS	Большой	0,752	Средний	Позитивное

В таблице 2 представлены средства поддержки при принятии решений для данных, передаваемых через WLAN, по сравнению с вероятными рисками. Злоумышленники могут попытаться найти уязвимости разными методами [24]. Существуют различные типы атак с шифрованием, как показано в Таблице 2, где уровень риска зависит от типа атаки. Следовательно, всестороннее изучение методов атаки является важной темой для выявления рисков с использованием предлагаемой модели. В этой таблице показаны соответствующие типы атак в соответствии с их методами и уровнем риска при применении методов обеспечения безопасности данных в подходящем и конфиденциальном режиме.

В таблице 3 представлена точность классификации пакетов с использованием наивного байесовского классификатора. Измерение энтропии используется как инструмент для проверки производительности полу-

Таблица 3.

Точность кластеризации предлагаемой системы

TP Rate*	FP** Rate	Точность	Отклик	F-мера	MCC	ROC Area	PRC Area	Уровень риска
0,973	0,007	0,955	0,937	0,946	0,937	0,997	0,986	Низкий
1.000	0,000	1.000	1,0000	1,0000	1.000	1,0000	1.000	Низкий
0,793	0,024	0,842	0,793	0,817	0,789	0,974	0,889	Средний
0,845	0,040	0,785	0,845	0,814	0,781	0,976	0,875	Средний
0,770	0,030	0,801	0,770	0,785	0,752	0,974	0,840	Высокий
0,970	0,010	0,946	0,970	0,958	0,950	0,998	0,991	Высокий
1.000	0,001	0,995	1.000	0,998	0,997	1.000	1.000	Очень Низкий
Взвешенное среднее	0,904	0,016	0,904	0,904	0,904	0,888	0,989	0,941

*TP Rate — истинно положительный результат
**FP Rate — ложный положительный результат

ченного классификатора, который обнаруживает набор пакетов в определенном кластере. Итак, если набор пакетов (M) принадлежит кластеру, то:

$$\text{Энтропия } (S) = -p+ \log_2 (p+) - p - \log_2 (p-) \qquad (7)$$

Производительность измеряется с точки зрения отклика модели и точности. Точность — это общее количество положительных классов, классифицированных соответствующим образом, разделенное на общее количество данных, отнесенных к категории положительных [25].

В качестве примера для проверки точности предлагаемой системы был использован пакет с открытым исходным кодом Weka для классификации и кластеризации данных на основе наивного байесовского классификатора со следующими характеристиками:

— количество экземпляров = 1500;
— многофакторный для всех атрибутов на основе региональной ориентации;
— тестовые операции: перекрестная проверка;
— формат выходного прогноза: CSV;
— кластеризация с использованием обучающего набора.

Результаты:

— минимум = 1;
— максимум = 254;
— среднее = 125,197;
— стандартное отклонение = 73,228.

Таким образом, приходим к выводу, что число (1356) правильно классифицированных случаев, что соответствует (90,4 %) уровню точности для средневзвешенного значения для всех возможных уровней риска, и (144) неправильно классифицированным случаям (т.е. 9,6 %) уровню точности. Уровень полноты и точности реализованной предложенной методики составляет 95 % с очень низким минимальным риском.

Таким образом, оптимизационная оценка уровня рисков является основным ключом к минимизации рисков посредством шифрования данных. В данной работе минимизация риска основана на предложенной системе шифрования. Предлагаемые модели основаны на этапах обучения, обучения и классификации, чтобы быть адаптируемыми и невосприимчивыми к различным атакам. Был использован пакет с открытым исходным кодом WEKA, основанный на простых байесовских классификаторах со специфическими функциями. Средний показатель точности составил 90,4 %. Отклик модели и число правильно классифицированных случаев отражают уровень точности, составивший 95 %, с очень низким минимальным риском.

ЛИТЕРАТУРА

1. Subramani M., Kumaravelu V.B. A fuzzy based vertical handover network selection scheme for device to device communication // Indonesian Journal of Electrical Engineering and Computer Science. 2020. Vol. 17. No. 1. Pp. 324–330.
2. Sulaiman M.S. Course recommendation system using fuzzy logic approach // Indonesian Journal of Electrical Engineering and Computer Science. 2020. Vol. 17. No. 1. Pp. 365–371.
3. Abdullah M.H. A. Evolving spiking neural networks methods for classification problem: a case study in flood events risk assessment // Indonesian Journal of Electrical Engineering and Computer Science. 2019. Vol. 16. No. 1. Pp. 222–229.
4. Ameur C. Intelligent optimization and management system for renewable energy systems using multi-agent // IAES International Journal of Artificial Intelligence (IJ-AI). 2019. Vol. 8. No. 4. Pp. 352–359.

5. Fallahpour A. A fuzzy decision support system for sustainable construction project selection: an integrated fpp-fis model // Journal of Civil Engineering and Management. 2020. Vol. 26. No. 3. Pp. 247–258.
6. Xin S. Research on Fuzzy Adaptive Intelligent Decision-making in Complex Environment // Journal of Physics: Conference Series. 2019. Pp. 3–12.
7. Ameen N. Comparative analysis of energy based optimized dynamic source multipath routing protocol in WSNs // Indonesian Journal of Electrical Engineering and computer Science. 2019. Vol. 16. No. 1. Pp. 441–455.
8. Hadzic O., Smajo B. Risk assessment for ancillary services // International Journal of Electrical and Computer Engineering (IJECE). 2019. Vol. 9. No. 3. Pp. 1561–1568.
9. Khan F. I. Security assessment of four open source software systems // Indonesian Journal of Electrical Engineering and Computer Science. 2019. Vol. 16. No. 2. Pp. 860–881.
10. Jupri M., Sarno R. Data mining, fuzzy AHP and TOPSIS for optimizing taxpayer supervision // Indonesian Journal of Electrical Engineering and Computer Science. 2020. Vol. 18. No. 1. Pp. 75–87.